

## REMARKS

1. Applicant thanks the Examiner for her remarks and observations which have greatly assisted Applicant in responding.
2. Applicant provides herewith an updated IDS with copies of all references cited.
3. **APPLICANT COMMENTS ON THE EXAMINER'S "RESPONSE TO ARGUMENTS" IN THE OFFICE ACTION OF MAY 31, 2007.**

Applicant notes the Examiner's comment that the slash in the expression "user id/client pair" indicates an alternative construction. Applicant finds the Examiner's comment inappropriate in view of the fact that the word "pair" clearly conveys that the elements "user ID" and "client" are both elements of the pair, and that no alternative interpretation is warranted.

Applicant notes the Examiner's comment that Olkin's teaching that a key and a message ID for the message that client wishes to send teaches "a client identifier." Applicant respectfully disagrees. A client identifier identifies the client. Olkin's key and message ID are associated to the message. They are therefore "message identifiers."

Applicant notes the Examiner's observation that creation of a message is an "instance of an application (where the client application is [a] software module which allows for email communications)." The foregoing observation makes little sense to Applicant. The ordinarily-skilled practitioner would understand "creation of a message" to be a function of an email client, not an instance. Furthermore, the ordinarily-skilled practitioner would understand that an "instance" of a software application (also known as an "instantiation") is a copy of the software application that is loaded into memory and being executed by a processor. The Examiner's rationale is completely opaque to Applicant. The comment, therefore, is without merit.

The Examiner asserts that Applicant's previous statement that Olkin provides no teaching of a trust token that includes a user ID or derivation thereof is incorrect, citing Olkin's ¶ 0051 as support. While ¶ 0051 mentions user ID fields, Olkin teaches that they are included in email send forms. An email send form is not a trust token.

The Examiner asserts that Applicant's previous statement that Olkin provides no teaching of encrypting a trust token is incorrect, citing ¶¶ 0115-0117 as support. What is described has nothing to do with a trust token as described in claim 1. The cited teaching describes sending an SSL message packet. However, the message packet is not a trust token, comprising only information related to the message and the user ID of the sender. There is no mention whatsoever of including a client ID in the SSL message. The present assertion is therefore without merit.

The Examiner asserts that Applicant's previous statement that Olkin provides no teaching of "transmitting a trust token from said network service to said client upon successful authentication to said network service by said entity" is incorrect. ¶ 0114 describes sending of a secure email. ¶ 0115 describes creation of record related to the sent message in the "sent mail table." There is no teaching or suggestion of sending of a trust token as described in claim 1.

The Examiner asserts that Olkin ¶¶ 0073-0076 teach "storing said issued trust token." The cited paragraphs describe a "user's table," "a user's alias table," and a "sent mail table." While the record in the "sent mail" table includes the message ID and the message key, as Applicant has previously explained, the message ID and the message key are associated to the message, not the client. Thus, they do not constitute a client ID as described in claim 1.

The remainder of the Examiner's remarks are equally lacking in merit, being based on the Examiner's faulty understanding of what constitutes a trust token. Any object or data structure described in Olkin is not a trust token unless it includes a client ID. While the Examiner may believe she has demonstrated that Olkin describes a client ID, she is incorrect. The client ID uniquely identifies the client. The Examiner, using the improper reasoning exposed above, has

determined that the message ID and/or the message key constitute a trust token as described in claim 1. They do not. The message key and/or the message ID are associated to the message, not to the client. Thus, they only identify the sent message. They do not uniquely identify the client. Because there is no teaching or suggestion anywhere of a client ID as described in claim 1, that uniquely identifies a client, not a message, there is no teaching or suggestion of a trust token, as described in claim 1, that includes a client ID.

**4. CLAIM OBJECTIONS**

Claims 3-4 and 33-34 are objected to because they depend from cancelled claims. Claim 3, 33 and 34 are cancelled from the Application, rendering the present objection moot. Claim 4 is amended to depend from claim 1. Accordingly, the present objection is overcome.

**5. 35 U.S.C. § 102**

Claims 1, 3-5, 8, 38, 40, 42, 45, 12-18, 30-31, 35, 49-65, 67-68 and 72 are rejected as being anticipated by U.S. publication no. 2003/0046533. As above, Applicant respectfully disagrees. Nevertheless, in the interest of advancing prosecution of the Application, claims 1 and 38 are amended to describe:

identifying entities legitimately entitled to service, wherein an entity comprises a user id-client pair, said user id-client pair comprising an individual user-machine combination;

establishing said identified entities as trusted entities by issuing a trust token for each entity successfully authenticating to said network service, said trust token comprising a data object that includes a client identifier, said client identifier comprising at least one item of data that can be used to uniquely identify the client machine, wherein a user ID-client pair represents a unique entity;

processing requests from said trusted entities according to a first policy;  
and

processing remaining requests according to at least a second policy.

Support for the amendments is found at least at ¶¶ 0022 and 0070 of U.S. publication no. 2005/0108551. As Applicant has previously emphasized, there is no teaching in Olkin of an entity constituting a user id-client pair. Applicant has amended claims 1 and 38, to describe the user id-client pair more clearly as an individual user-machine combination. Application further describes the client ID as at least one item of data that can be used to uniquely identify the client machine, wherein a user ID-client pair represents a unique entity. There is no such teaching in Olkin. Accordingly, there is no anticipation. Therefore, even if the rejection of claims 1 and 38 were not improper, the present amendment to claims 1 and 38 renders them allowable under 35 U.S.C § 102.

In view of their dependence from allowable parents, the dependent claims are deemed allowable without any separate consideration of their merits.

**6. 35 U.S.C. § 103**

Claims 9 and 46 are rejected as being unpatentable over Olkin in view of U.S. publication no. 2002/0052921 ("Morkel"). In view of the foregoing amendment to claims 1 and 38, the present rejection is deemed overcome.

Claims 10, 29, 37, 47, 66 and 74 are rejected as being unpatentable over Olkin in view of U.S. publication no. 2003/0028495 ("Pallante"). In view of the foregoing amendment to claims 1 and 38, the present rejection is deemed overcome.

Claims 32-33, 36, 69-70 and 73 are rejected as being unpatentable over Olkin in view of U.S. publication no. 2002/0042883 ("Roux"). In view of the above amendment to claims 1 and 38, the present rejection is deemed overcome.

Claims 34 and 71 are rejected as being unpatentable over Olkin in view of U.S. publication no. 2003/0046533 ("Card"). In view of the foregoing amendment to claims 1 and 38, the present rejection is deemed overcome.

Claims 75-76, 78-87 and 93 are rejected as being unpatentable over Olkin in view of Pallante. To describe the invention more clearly, Applicant amends claim 75 to incorporate the subject matter of claims 87 and 88:

“processing requests from trusted entities according to a first policy; and processing remaining requests according to at least a second policy, wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing untrusted logins.” There is no teaching of such subject matter in the combination of Olkin and Pallante. Accordingly, the present rejection is deemed overcome.

The subject matter of claim 88 is rejected as being unpatentable over Olkin in view of Pall ante and further in view of Roux. Applicant respectfully disagrees. The Examiner relies on Roux, ¶ 0047 as teaching or suggesting “wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing untrusted logins.” Applicant respectfully disagrees.

Applicant first notes that the Examiner’s interpretation of what Roux, ¶ 0047 teaches is incorrect. The Examiner suggests the cited paragraph teaches that a response should be received within a valid period of time in order to determine whether or not a certain user is trustworthy. What the cited paragraph actually describes is:

“Within the security server there is provided a stack monitor 41 to monitor the flow of IP traffic into and out of the security server. When the stack monitor 41 detects a flag in an IP acknowledgement from a client, a profile request generator 45 can control the stack monitor 41 to request a profile from the client. When the profile is received, a validation request generator 44 can control the stack monitor 41 to send the profile together with the request for validation to the secure server 50. If no flag is set in the IP acknowledgement from the IP client, a profile is not received from the IP client, or the validation response from the secure server indicates the profile is invalid, a default response generator 43 can generate a default response that is sent to the client. The default response can either be a message or data. For example, the default response can comprise HTML for a web page, or simply a referral to another web site. This will cause the web browser within the client to display a web page, thus masking the fact that access has been denied to the target server.”

Thus, if a client cannot, or does not provide a valid profile, the security server stereotypically denies access to the client. Thus, there is no teaching in Roux of "adding a configurable amount of incremental response latency when processing untrusted logins". Accordingly, there is no teaching or suggestion of the subject matter of claim 88 in the combination of Olkin, Pall ante and Roux.

Even if the Examiner's interpretation of the Roux teachings were not incorrect, a mere suggestion that trusted traffic should arrive within a certain period of time does not constitute a teaching or suggestion of adding a configurable amount of incremental response latency when processing untrusted logins.

Claims 77, 89-91 and 94 are additionally rejected as being unpatentable over the combination of Olkin, Pall ante and Roux. In view of the foregoing, the present rejection is deemed overcome.

Claim 92 is rejected as being unpatentable over Olkin in view of Pall ante and further in view of Card. In view of the above amendment to claim 75, the present rejection is deemed overcome.

7. No new matter is added by way of the above amendments. Additional amendments have been made to the dependent claims to bring them into harmony with the independent claims. No new matter is added by way of these amendments.

The foregoing amendments are made in the interest of advancing prosecution of the Application. They do not signify agreement with the Examiner's position. Nor do they reflect intent to sacrifice claim scope. Applicant expressly reserves the right to pursue protection of a scope it reasonably believes it is entitled to in one or more continuing submissions to the USPTO.

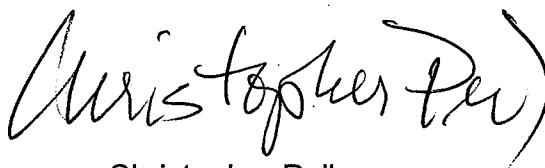
8. For the record, Applicant respectfully traverses any and all factual assertions in the file that are not supported by documentary evidence. Such include assertions based on findings of inherency, assertions based on official

notice, and any other assertions of what is well known or commonly known in the prior art.

### CONCLUSION

In view of the foregoing, the Application is deemed to be in allowable condition. Therefore, Applicant respectfully requests reconsideration and prompt allowance of the claims. Should the Examiner have any questions regarding the Application, he is urged to contact Applicant's Attorney at 650-474-8400.

Respectfully submitted,

A handwritten signature in black ink, reading "Christopher Peil". The signature is written in a cursive, flowing style with a large, stylized "C" and "P".

Christopher Peil

Reg. No. 45,005

Customer No. 22862